BAB II
LANDASAN TEORI

2.1. Jaringan Komputer

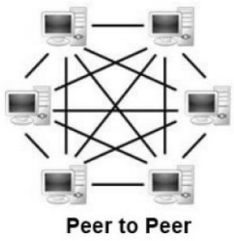
Jaringan komputer adalah himpunan "interkoneksi" antara 2 komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless).* Bila sebuah komputer dapat membuat komputer lain *restart*, shutdown, atau dapat melakukan control lainnya, maka computer-komputer tersebut bukan *autonomous* (tidak melakukan kontrol terhadap komputer lain dengan akses penuh).

Tiap komputer, printer atau perangkat yang terhubung dalam suatu jaringan disebut denga ***node.*** Sebuah jaringan komputer sekurang-kurangnya terdiri dari dua unit komputer atau lebih, dapat berjumlah puluhan komputer,ribuan atau bahkan jutaan node saling terhubung satu dengan lainnya. (Syafrizal, 2005)

Di dalam jaringan komputer dikenal dengan sistem koneksi antarnode (*computer*), yakni:

2.1.1. Peer to Peer

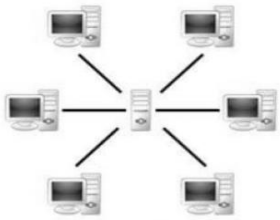
Peer to peer adalah suatu model di mana setiap PC (*Personal Computer)* dapat memakai sumber daya pada PC lain atau memberikan sumber dayanya untuk dipakai komputer lain. Dengan kata lain dapat berfungsi sebagai *client* maupun *server* pada waktu yang sama.



Gambar 2.1 Jaringan Peer to Peer (Syafrizal, 2005)

2.1.2. Client - Server

Dimana ada satu unit komputer berfungsi sebagai *server* yang hanya memberikan layanan bagi komputer lain, dan *client* yang juga hanya meminta layanan dari *server*. Akses dilakukan secara transparent dari *client* dengan melakukan login terlebihh dulu ke *server* yang dituju.

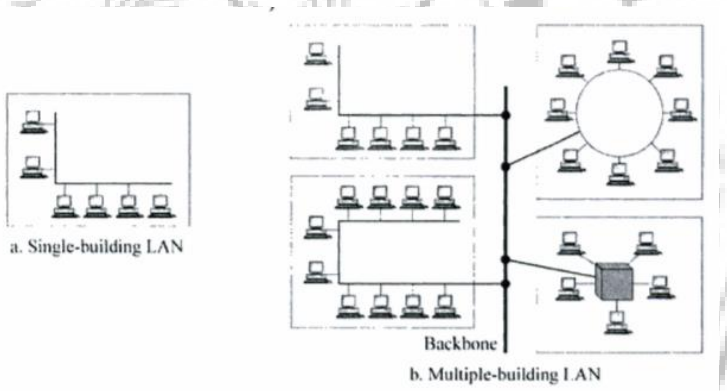


Gambar 2.2 Client-Server (Syafrizal, 2005)

Sedangkan menurut jenisnya jaringan komputer secara umum ada 3 macam yaitu :

2.1.3. LAN (Local Area Network)

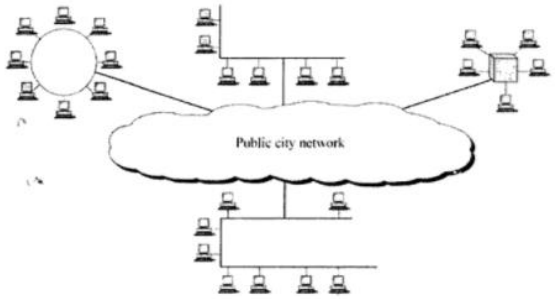
Sebuah LAN adalah jaringan yang dibatasi oleh area yang relatih kecil, umumnya dibatasi oleh area lingkungan, seperti sebuah kantor pada sebuah gedung, atau tiap-tiap ruagan pada sebuah sekolah. Biasanya jarak antarnode tidak lebih jauh dari sekitar 200 m.



Gambar 2.3 Local Area Network (Syafirzal, 2005)

2.1.4. MAN (Metropolitan Area Network)

Sebuah MAN bisanya meliputi area yang lebih besar dari LAN, misalnya antar gedung dalam satu daerah (wilayah seperti propinsi atau Negara bagian) meng. Dalam hal ini jaringan menghubungkn beberapa buah jarigan kecil kedalam lingkungan area yang lebih besar. Sebagai contoh jaringan beberapa kantor cabang sebuah bank di dalam sebuah kota besar yang dihubungkan antara satu dengan lainnya.



Gambar 2.4 Metropolitan Area Network (Syafirzal, 2005)

2.1.5. WAN (Wide Area Network)

WAN adalah jaringan yang biasanya sudah menggunakan media *wireless*, sarana satelit, ataupun kabel serat optic, karena jangkauannya yang lebih luas, bukan hanya meliputi satu kota atau antarkota dalam suatu wilayah, tetapi mulai menjangkau area / wilayah otoritas negara lain.

Gambar 2.5 Wide Area Network (Syafirzal, 2005)

Tabel 2.1 Interkoneksi berdasarkan jarak antar *node*

Jarak antarkomputer	Lokasi/Area	Jenis Jaringan
1 – 10 m	Ruangan	Local Area Network
100 m - < 1 km	Gedung perkantoran	
1 – 10 km	Kota	Metropolitan Area Network
> 10 - < 100 km	Kabupaten, Propinsi	
>= 100 km	Negara	Wide Area Network
>= 1.000 km	Benua	
>= 10.000 km	Planet	Internet

Menurut Syafrizal (2005) , “ Nilai – nilai yang terdapat pada table diatas bukan merupakan nilai mutlak bagi jarak yang menghubungkan antar komputer , karena jarak tersebut bisa saja lebih pendek atau lebih panjang, tergantung pada kondisi area suatu wilayah. “

2.2. Virtual Private Network

Menurut Utomo (2015) *Virtual Private Network* (VPN) adalah sebuah teknologi komunikasi yang memungkinkan dapat terkoneksi ke jaringan public dan menggunaannya untuk dapat bergabung dengan jaringan lokal. VPN merupakan koneksi virtual yang bersifat *private*, dikarenakan jaringan yang dibuat tidak nampak secara fisik hanya berupa jaringan virtual dan jaringan tersebuat tidak semua orang dapat mengaksesnya sehingga sifatnya *private*. Dengan cara tersebuat maka akan didapatkan hak dengan pengaturan yang sama seperti halnya berada didalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunkan jaringan milik public.

Teknologi VPN menyediakan beberapa fungsi utama untuk penggunaanya. Fungsi-fungsi utama tersebut antara lain sebagai berikut.

a. *Confidentially* (Kerahasiaan)

Dengan digunakannya jaringan public yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data lebih terjaga.

b. *Data Intergrity* (Keutuhan Data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai Negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang,rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data diterima.

c. *Origin Authentication* (Auntentifikasi Sumber)

VPN akan melakukan pemeriksaaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses auntentifikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

d. Non-repuditon

Yaitu mencegah dua pihak dari menyangkal bahwa mereka telah mengirim atau menerima sebuah *file* mengakomodasi perubahan.

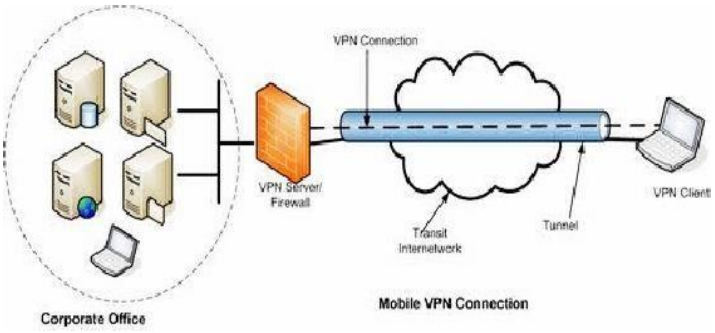
e. Kendali Akses

Menentukan siapa yang diberikan akses ke sebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima`

2.3. Konsep VPN

Jaringan VPN menawarkan keamanan dan tidak terdeteksi dikarenakan IP yang digunakan berupa IP Public milik VPN *server*. Dengan adanya enkripsi dan dekripsi, maka data yang melalui jaringan internet ini tidak dapat diakses oleh orang lain bahkan oleh *client* lain yang terhubung dengan *server* VPN. Kunci yang dibutuhkan untuk membuka enkripsi tersebut hanya diketahui oleh *server* VPN dan *client* yang terhubung dengannya. Dengan penggunaan enkripsi dan dekripsi itulah yang menyebabkan data yang melalui jaringan tidak dapat modifikasi dan dibaca sehingga keamanannya terjamin Hendriana (2012).

tersebut didukung oleh salah satu lembaga internet IETF (*Internet Engineering Task Force)* menjelaskan bahwa *" VPN is an emulation of a private Wide Area Network (WAN) using shared or public IP facilities, such as the Internet or private IP backbones".* Dimana *VPN* merupakan suatu bentuk *private* internet yang melalui jaringan publik (internet), dengan menitik beratkan pada keamanan data dan akses global melalui internet. Hal ini dibangun melalui suatu *tunnel* (terowongan) virtual antara 2 node. suatu jaringan *private* (biasanya untuk instansi atau kelompok tertentu) di dalam jaringan internet publik, dimana jaringan privat ini seolah-olah sedang mengakses jaringan lokalnya tapi menggunakan jaringan publik.



Gambar 2.6 Konsep VPN (Ardiyansyah, 2008)

2.4.Jenis Implementasi VPN

- *Remote Access* VPN

Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah *remote access* VPN, dan yang kedua adalah site-to-site VPN. *Remote access* yang biasa juga disebut virtual *private dial-up network* (VPDN), menghubungkan antara pengguna yang mobile dengan local area network (LAN).

Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan software klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.

Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-dial nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *software* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan remote access VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP (Ardiansyah, 2008).

- *Site-to-site* VPN

Jenis implementasi VPN yang kedua adalah site-to-site VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet site-to-site VPN (Ardiansyah, 2008)

2.5. Protokol dan Teknologi VPN

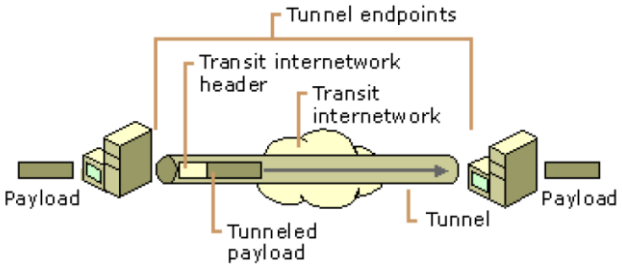
Beberapa protokol network yang menarik telah diimplementasikan untuk penggunaan VPN. Protokol-protokol ini mencoba untuk menutup beberapa hole sekuritas bawaan dalam VPN. Protokol-protokol ini pun melanjutkan untuk bersaing dengan lainnya dalam hal penerimaan dunia industri. Beberapa protokol network mulai populer sebagai efek pengembangan VPN diantaranya adalah :

a. PPTP (Point-to-point Tunneling Protocol)
b. L2TP (Layer Two Tunneling Protocol)
c. IPsec (Internet Protocol Security)
d. SOCKS Network Security Protocol

2.5.1. *Point-to-Point Tunneling Protocol* (PPTP)

PPTP merupakan protokol jaringan yang dikembangkan oleh Microsoft dan Cisco yang memungkinkan pengamanan transfer data dari *remote client* ke *server* pribadi instansi dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan yang terdapat pada PPTP adalah pengembangan dari *remote access Point-to-Point Protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP membungkus paket PPP menjadi IP *datagrams* agar dapat ditransmisikan melalui internet atau jaringan publik berbasis TCP/IP. PPTP juga dapat digunakan pada jaringan *private LAN-toLAN* (Utomo, 2015).

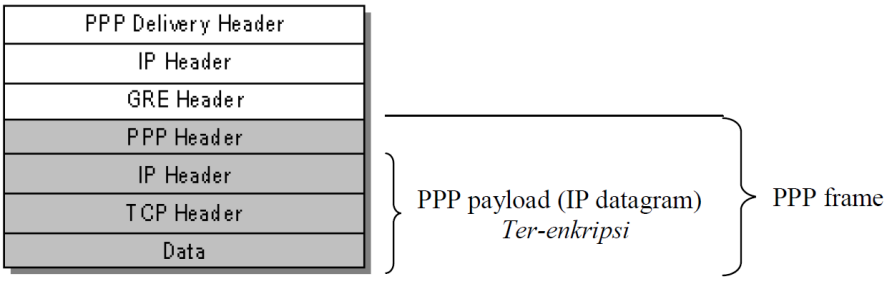
Seluruh komunikasi data antar jaringan pribadi akan melalui *tunnel* ini, sehingga orang atau user dari jaringan publik yang tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak atau mencuri data yang melintasi tunnel ini. Di dalam tunneling terdapat proses enkapsulasi, transmisi dan dekapsulasi paket yang di komunikasikan. Metode tunneling dapat digambarkan secara ringkas sebagai berikut:



Gambar 2.7 Metode *Tunneling* (Ramadhan, 2014)

Teknologi tunneling dikelompokkan secara garis besar berdasarkan protokol tunneling layer 2 (Data Link Layer) dan layer 3 (Network Layer) model OSI layer. Yang termasuk ke dalam tunneling layer 2 adalah L2F, PPTP, dan L2TP. Sedangkan yang termasuk layer 3 adalah IPSec, VTP, dan ATMP.

Setelah PPTP tunnel terbentuk, data dari user ditransmisikan antara PPTP client dan PPTP server. Data yang ditransmisikan dalam bentuk IP datagram yang berisi PPP paket. IP datagram dibuat dengan menggunakan versi protokol Generic Routing Encapsulation (GRE) internet yang telah dimodifikasi. Struktur paket data yang dikirimkan melalui PPTP dapat digambarkan sebagai berikut:

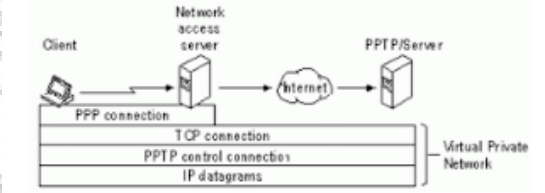


Gambar 2.8 Paket data PPTP (Ramadhan, 2014)

Cara kerja PPTP dimulai dari sebuah remote atau PPTP client mobile yang membutuhkan akses ke sebuah LAN private dari sebuah perusahaan. Pengaksesan dilakukan dengan menggunakan ISP lokal. Client (yang menggunakan *Windows*

NT Server versi 4.0 atau Windows NT Workstation versi 4.0) menggunakan Dial-Up networking dan protokol remote access PPP untuk terhubung ke sebuah ISP. Client terhubung ke Network Access Server (NAS) pada fasilitas ISP. NAS di sini bisa berupa prosesor *front-end*, server dial-in atau *server Point-of-Presence* (POP). Begitu terhubung, client bisa mengirim dan menerima paket data melalui internet. NAS menggunakan protocol TCP/IP untuk semua trafik yang melalui internet

Setelah client membuat koneksi PPP ke ISP, panggilan *Dial-Up Networking* yang kedua dibuat melalui koneksi PPP yang sudah ada. Data dikirimkan menggunakan koneksi yang kedua ini dalam bentuk IP datagram yang berisi paket PPP yang telah ter-enkapsulasi. Panggilan yang kedua tersebut selanjutnya menciptakan koneksi VPN ke server PPTP pada LAN private perusahaan. Koneksi inilah (melalui panggilan kedua) yang di-istilahkan sebagai *tunnel* (lorong). Berikut ini gambar yang menjelaskan proses tersebut :



Gambar 2.9 *Tunnel* PPTP (Ramadhan, 2014)

Tunneling pada gambar diatas adalah sebuah proses pengiriman paket data ke sebuah komputer pada jaringan privat dengan me-routing paket data tersebut melalui beberapa jaringan yang lain, misalnya Internet. Router-router jaringan yang lain tidak bisa mengakses komputer yang berada pada jaringan privat. Oleh karena itu, tunneling memungkinkan jaringan routing untuk mentransmisikan paket data ke komputer penghubung, seperti PPTP *server*, yang terhubung ke jaringan *routing* dan jaringan *private*. PPTP client dan PPTP *server* menggunakan tunneling untuk merutekan paket data secara aman ke komputer yang berada pada jaringan privat melalui router-router yang hanya mengetahui alamat *server* penghubung jaringan *privat*e. (Ramadhan, 2014)

2.5.2. *Layer* 2 *Tunneling* Protocol (L2TP)

Menurut Utomo (2015) L2TP merupakan *tunneling protocol* yang memadukan dua buah tunneling protokol yaitu *Layer* 2 *Forwarding* milik Cisco

dan PPTP yang dimiliki Microsoft. L2TP umumnya digunakan untuk membuat Virtual Private Dial Network (VPDN) yang dapat membawa semua jenis protokol komunikasi di dalamnya dan biasanya menggunakan port 1702 dengan protokol UDP. Terdapat dua model tunnel yang dikenal, yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint* tunnel-nya. Pada *compulsory tunnel,* ujung *tunnel* berada pada ISP, sedangkan pada *voluntary* ujung *tunnel* berada pada *client remote*.

2.5.3. *Internet Protocol Security* (IPSec)

IPSec adalah pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan *layer* yang berada diatasnya. Pada dasarnya paket IP tidak memiliki keamanan, sehingga tidak ada jaminan bahwa paket yang diterima sama dengan paket ketika ditransmisikan oleh si pengirim paket. Paket IP yang tidak memiliki keamanan atau *security,* sangat mudah untuk diketahui isinya dan alamat IP itu sendiri. IPsec adalah metode yang bertujuan untuk menjaga keamanan IP datagram ketika paket diransmisikan pada *traffic*. Sehingga IPsec menjadi suatu mekanisme yang diimplementasikan pada VPN. *IPSec* berada pada *layer* tiga OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada atasnya. IPSec terdiri dari dua buah *security* protokol :

- *AH* (*Authentication Header*) melakukan autentikasi datagram untuk mengidentifikasi pengirim data tersebut.
- *ESP* (*Encapsulating Security Header*) melakukan enkripsi dan layanan autentifikasi.

Dua buah protokol tersebut dapat dikombinasikan atau berdiri sendiri dalam penyediaan kemanan. IPSec menggunakan dua buah protokol berbeda untuk menyediakan pengamanan data yaitu *AH* dan *ESP* keduanya dapat dikombinasikan ataupun berdiri sendiri. Dengan menggunakan IPSec maka suatu sistem dapat memilih protokol security apa yang akan digunakan, dikarenakan IPsec berada pada level IP (Utomo, 2015).

2.5.4. SOCKS Network Security Protocol

Sistem SOCK menyediakan sebuah alternatif unik ke protokol VPN lainnya. Fungsi SOCKS pada layer session (layer 5) dalam OSI, membandingkan semua protokol VPN lainnya yang bekerja pada layer 2 atau 3. Implementasi ini menawarkan keuntungan sekaligus kerugian melalui pilihan-pilihan protokol lainnya tersebut. Fungsi pada level yang lebih tinggi, SOCKS mengizinkan administrator untuk membatasi trafik VPN untuk aplikasi tertentu saja. Untuk menggunakan SOCKS, administrator harus mengkonfigurasikan SOCKS proxy server dalam lingkungan client seperti software SOCKS pada client itu sendiri (Suryani & Honey, 2006).

2.6. OpenVPN

Gambar 2.10 Logo OpenVPN

OpenVPN adalah sebuah solusi VPN antar *platform* , aman dan sangat mudah dikonfigurasikan dengan menggunakan *intervface* virtual yang disediakan oleh *driver* jaringan universal TUN / TAP dan dijalankan sepenuhnya oleh pengguna yang merupakan perlindungan khusus pada sistem.

Keputusan ini dibuat untuk menyediakan keamanan yang lebih baik, karena jika sebuah celah ditemukan oleh penyusup maka aksesnya akan menjadi terbatas. OpenVPN mendukung konfigurasi *peer-to-peer* dan multiclient yang memungkinkan untuk membuat banyak topologi VPN seperti : *host-host* , *hostnetwork* dan *network-network*. Hal ini mendukung untuk menciptakan VPN layer 3 atau layer 2 dengan menggunakan antar muka TUN / TAP.

OpenVPN membuat sebuah SSL/TLS *session* untuk *control channel* antar *peer*, selama fase autentifikasi tiap *peer* melakukan pertukaran sertifikasi yang di tanda tangani oleh CA (*certificate of Authority*) yang saling di percaya. Setelah

autentikasi selesai dan SSL *session* telah terbangun di tiap *peer* , OpenVPN menggunakan koneksi, melakukan negosiasi kunci untuk data channel (Utomo, 2015).

2.7. Ubuntu

Gambar 2.11 Logo Ubuntu

Ubuntu berasal dari bahasa kuno Afrika, yang berarti "rasa perikemanusian terhadap sesama manusia". Ubuntu juga bisa berarti "aku adalah aku karena keberadaan kita semua". Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam Ubuntu ke dalam dunia perangkat lunak.

Ubuntu adalah sistem operasi lengkap berbasis Linux, tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional. Ubuntu sendiri dikembangkan oleh komunitas sukarelawan Ubuntu dan kami mengundang Anda untuk turut serta berpartisipasi mengembangkan Ubuntu.

Komunitas Ubuntu dibentuk berdasarkan gagasan yang terdapat di dalam filosofi Ubuntu: bahwa perangkat lunak harus tersedia dengan bebas biaya, bahwa aplikasi perangkat lunak tersebut harus dapat digunakan dalam bahasa lokal masing-masing dan untuk orang-orang yang mempunyai keterbatasan fisik, dan bahwa pengguna harus mempunyai kebebasan untuk mengubah perangkat lunak sesuai dengan apa yang mereka butuhkan .Perihal kebebasan inilah yang membuat Ubuntu berbeda dari perangkat lunak berpemilik (proprietary); bukan hanya peralatan yang Anda butuhkan tersedia secara bebas biaya, tetapi Anda juga mempunyai hak untuk memodifikasi perangkat lunak Anda sampai perangkat lunak tersebut bekerja sesuai dengan yang Anda inginkan (Ubuntu Indonesia)

Berikut ini adalah komitmen publik tim Ubuntu untuk para penggunanya:

- Ubuntu akan selalu bebas dari biaya, maka dari itu tidak akan ada biaya tambahan untuk "edisi enterprise", kami akan membuat semua pekerjaan terbaik Ubuntu tersedia untuk semua orang dengan istilah Bebas yang sama.
- Ubuntu juga menyediakan dukungan komersial dari ratusan perusahaan di seluruh dunia. Ubuntu dirilis secara tetap dan dapat Anda prediksikan; rilis Ubuntu terbaru tersedia setiap enam bulan. Setiap rilis akan didukung oleh Ubuntu dengan perbaikan pada keamanan dan perbaikan lainnya secara bebas selama sekurangnya 18 bulan.
- Ubuntu akan menyertakan terjemahan dan prasarana aksesibilitas terbaik yang dimiliki oleh komunitas Perangkat Lunak Bebas, hal ini berguna untuk membuat Ubuntu dapat dipergunakan oleh banyak orang. Kami juga bekerja sama dengan seluruh komunitas Perangkat Lunak Bebas dalam hal perbaikan bug dan saling membagi kode.
- Ubuntu berkomitmen secara penuh terhadap prinsip-prinsip dari pengembangan perangkat lunak bebas; untuk ini kami mendorong masyarakat untuk menggunakan perangkat lunak bebas dan open source, lalu memperbaikinya dan kemudian menyebarkannya kembali.

Ubuntu cocok digunakan baik untuk desktop maupun server. Ubuntu saat ini mendukung berbagai arsitektur komputer seperti PC (Intel x86), PC 64-bita (AMD64), PowerPC (Apple iBook dan Powerbook, G4 dan G5), Sun UltraSPARC dan T1 (Sun Fire T1000 dan T2000).

Ubuntu menyertakan lebih dari 16.000 buah perangkat lunak, dan untuk instalasi desktop dapat dilakukan dengan menggunakan satu CD saja. Ubuntu menyertakan semua aplikasi standar untuk desktop mulai dari pengolah kata, aplikasi lembar sebar (spreadsheet) hingga aplikasi untuk mengakses internet, perangkat lunak untuk server web, peralatan untuk bahasa pemrograman dan tentu saja beragam permainan.

2.8. Ubuntu Server

Linux Ubuntu Server adalah sistem operasi turunan dari Linux Ubuntu yang di desain khusus dengan kernel yang telah dikustomisasi untuk bekerja sebagai sistem operasi Server. Kernel Linux Ubuntu Server di desain khusus untuk bisa

bekerja dengan lebih dari satu proses (multiprocessor) dengan dukungan NUMA pada 100Hz internal timer frequency dan menggunakan penjadwalan deadline I/O.

Linux Ubuntu Server memiliki lisensi open source dan gratis serta merupakan turunan dari distro linux debian sehingga memiliki keamanan yang cukup tinggi. Selain itu, setiap bugs yang berkaitan dengan keamanan cepat ditangani oleh Tim keamanan Linux Ubuntu yang bekerja sama dengan Tim keamanan debian.

Linux Ubuntu Server memiliki kebutuhan minimum atau resource yang harus dipenuhi diantaranya adalah prosesor 300 MHz, Memory 64MB, Hardisk 500MB, dan VGA 640×480. Namun, untuk menjalankan aplikasi dengan komputasi yang cukup besar maka sebaiknya resource pada komputer disediakan lebih tinggi untuk meningkatkan kinerja pada aplikasi.

Kelebihan :

- Freeware yaitu software yang bersifat free tanpa ada tuntutan dari hak cipta.
- Kita bisa mencoba menggunakan Ubuntu tanpa perlu menginstalnya kedalam harddisk komputer, dengan menggunakan fitur Live CD pada Ubuntu melalui proses boot pada CD atau flashdisk saja.
- Start / shutdown cepat.
- Tahan virus.
- Terdapat lebih dari 55 bahasa, termasuk bahasa Indonesia. Sehingga memudahkan anda dalam menggunakan Ubuntu, jika anda tak mengerti bahasa Inggris.
- Tidak begitu membutuhkan hardware yang terlalu besar kapasitasnya maupun biayanya.
- Akses data full proteksi dari pengguna.

Kekurangan :

- Struktur direktori dan hak-akses yang membingungkan bagi yang sudah terbiasa dengan Windows dan belum mengenal UNIX/Linux sama sekali.
- Proses instalasi agak lama karena paket yang di install harus update secara online.

- Belum user friendly, dikarena sebagian besar pengguna Ubuntu berasal dari migrasi Windows dan lainnya

2.9. MikroTik

Gambar 2.12 Logo MikroTik

MikroTik adalah perusahaan kecil yang berkantor pusat di Latvia, dibentuk oleh John Trully dan Arnis Riekstins. Pada tahun 1996 John dan Arnis memulai dengan sistem Linux dan MS DOS yang dikombinasikan dengan teknologi Wireless LAN (W-LAN). MikroTik memliki system perangakat lunaknya sendiri yaitu MikroTik RouterOS . **MikroTikRouterOS™** merupakan sistem operasi yang diperuntukkan sebagai network router.

MikroTik routerOS sendiri adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan *wireless*. Fitur-fitur tersebut diantaranya: Firewall & Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, Hotspot, dan masih banyak lagi fitur lainnya. MikroTik routerOS merupakan sistem operasi Linux base yang diperuntukkan sebagai network router.

Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada Standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan sumber daya PC yang memadai. Ini adalah versi

MikroTik dalam bentuk perangkat lunak yang dapat dipasang pada komputer rumahan (PC) melalui CD *File image* MikroTik

RouterOS bisa diundug dari website resmi MikroTik,www.mikrotik.com. Namun, file image ini merupakan versi *trial* MikroTik yang hanya dapat digunakan dalam waktu 24 jam saja. Untuk dapat menggunakannya secara *full time*, anda harus membeli *lisensi key* dengan catatan satu lisensi hanya untuk satu harddisk. Mikrotik RouterOS hadir dalam berbagai level dan tiap levelnya memiliki kemampuannya masing-masing, mulai dari level 3 hingga level 6. Secara singkat, level 3 digunakan untuk router berinterface ethernet, level 4 digunakan untuk jaringan wireless client atau serial interface, level 5 digunakan untuk jaringan wireless Access Point, dan level 6 tidak mempunyai limitasi apapun. Untuk aplikasi hotspot, bisa menggunakan level 4 dengan kapasitas 200 pengguna atau level 5 dengan kapasitas 500 pengguna atau untuk coveragge yang luas, bisa menggunakan level 6 yang kapasitasnya tidak terbatas (Khasanah, 2015).

2.10. Winbox

Gambar 2.13 Logo Winbox

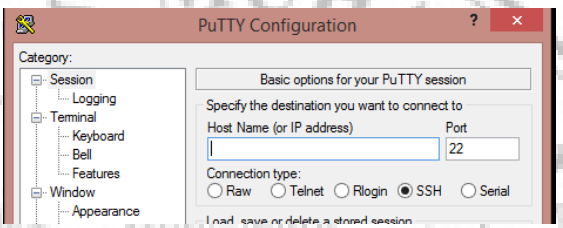
Winbox Loader merupakan aplikasi yang digunakan untuk remote router mikrotik, aplikasi ini dapat membaca mac address mikrotik, jadi saat mikrotik belum dikonfigurasi *IP*-nya d engan aplikasi ini tetap dapat digunakan dengan membaca *mac address* yang ada di *interface* mikrotik .

2.11. WinSCP

Gambar 2.14 Logo WinSCP (Mundianarti, 2017)

WinSCP merupakan aplikasi SSH *Client* berbasis sistem operasi Windows yang bersifat open source. Fokus utama WinSCP adalah mengirim file ke remote komputer (server) menggunakan port SSH yang lebih aman. Dengan demikian, WinSCP juga merupakan sebuah aplikasi SFTP *client*, SCP *client* dan FTP *Client*. Dimana Kegunaan dari WinSCP ini adalah sebagai alat untuk transfer, atau lebih familiar kita kenal dengan sebutan upload dan download file melalui protokol ftp dan secure shell (SSH), Dengan WinSCP kita juga dapat melakukan editorial seperti mengedit isi file, merubah nama file menghapus file serta membuat folder dan file baru atau perbaikan terhadap teks sebuah file (Mundianarti, 2017).

2.12. PuTTY



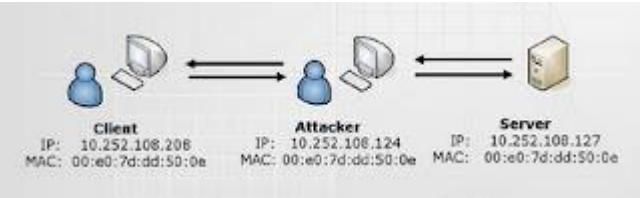
Gambar 2.15 Tampilan PuTTY (Kusumawati, 2017).

PuTTY merupakan perangkat lunak yang berfungsi sebagai terminal *emulator* pada area *Telnet, Rlogin, SSH,* maupun *Serial communications.* Fungsi mendasar dari aplikasi ini tentu saja untuk menggabungkan jaringan,sehingga jaringan bisa berjalan pada *host* yang tersedia. *User* bisa memanfaatkan *PuTTY* agar bisa terhubung dengan perangkat penghubung misalnya *switch* atau *hub.*

Aplikasi ini akan memungkinkan pengguna untuk melakukan transfer dan terima data melalui SFTP atau *Secure Shell File Transfer Protokol* (Kusumawati, 2017).

2.13. Sinffing

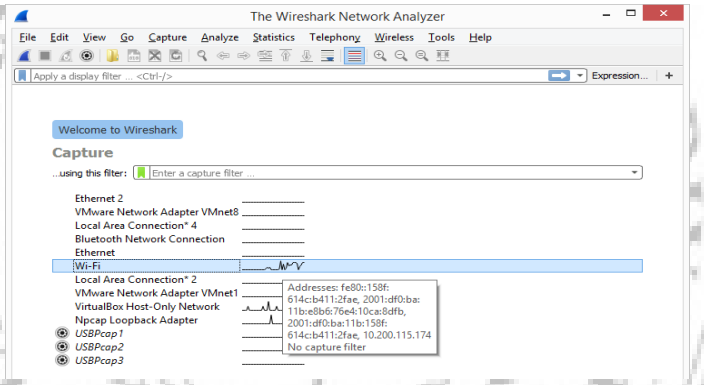
Sniffing adalah aktivitas menyadap paket data yang sedang berjalan pada *traffic* sebuah jaringan. Paket data ini bisa berisi informasi mengenai apa saja, baik itu username, apa yang dilakukan pengguna melalui jaringan, termasuk mengidentifikasi komputer yang terinfeksi virus, sekaligus melihat apa yang membuat komputer menjadi lambat dalam jaringan. *Sniffing* juga dapat mengidentifikasi penyebab macet pada jaringan (Utomo, 2015).



Gambar 2.17 Ilustrasi *Sniffing* (Viani, 2012)

2.14. WireShark

Wireshark merupakan *Network Packet Analyzer*. Network Packet Analyzer akan mencoba menangkap paket-paket jaringan dan berusaha untuk menampilkan informasi tersebut sedetail mungkin. *Network Packet Analyzer* diibaratkan sebagai *tool* untuk memeriksa apa yang sebenarnya terjadi di dalam sebuah jaringan. Wireshark merupakan salah satu tool gratis terbaik untuk menganalisa paket jaringan. (Khairina, 2011).



Gambar 2.18 Tampilan Wireshark

2.15. VirtualBox

Gambar 2.19 Logo VirtualBox

VirtualBox adalah *software* virtualisasi, digunakan untuk menjalankan sistem operasi tambahan di dalam sistem operasi utama. atau bisa disebut sebagai wadah

untuk simulasi sebuah sistem operasi. VirtualBox merupakan mesin virtual yang digunakan jika kita ingin menginstal atau mencoba sebuah sistem operasi di komputer kita. (Setiawan, 2015)

Fungsi VirtualBox :

- Mencoba sistem operasi yang baru rilis atau masih dalam tahap uji
- Mencoba sistem operasi yang berbeda dengan sistem operasi utama
- Mencoba simulasi menguji sebuah security, entah itu sistem operasi bahkan website dan
- Mencoba untuk membuat sebuah simulasi jaringan